

**We Claim as Our Invention:**

1. A user authentication system, comprising:
  - a data holding medium for holding a common key unique to a user, used in a common-key encryption method;
  - 5 an authentication apparatus for holding the common key used in the common-key encryption method and a private key used in a public-key encryption method, each unique to the user; and
  - an information processing apparatus connected to the authentication apparatus in an always-communicable manner and provided with a function for
  - 10 performing authentication by the public-key encryption method;
  - wherein the authentication apparatus performs authentication by using the common key held by the data holding medium and the common key held by the authentication apparatus, in response to a user authentication request sent from the information processing apparatus, and, only when the user has been authenticated,
  - 15 performs processing for making the information processing apparatus authenticate the user by using the private key corresponding to the user.
2. An authentication system as claimed in Claim 1, wherein the data holding medium is portable.
- 20 3. An authentication system as claimed in Claim 1, wherein the information processing apparatus is a mobile communication apparatus.
4. An authentication system as claimed in Claim 1, wherein the data holding medium and the information processing apparatus are integrated as a unit.
- 25 5. A user authentication method for a user who carries a data holding apparatus for holding a common key used in a common-key encryption method, the method comprising the steps of:
  - 30 authenticating the user by the common-key encryption method by using the common key held by the data holding apparatus of the user in response to a user authentication request; and

performing, only when the user has been authenticated, processing for authenticating the user by a public-key encryption method.

6. A user authentication method as claimed in Claim 5, wherein the data  
5 holding medium is portable.

7. A user authentication method as claimed in Claim 5, wherein the user authentication request is sent from an information processing apparatus.

10 8. A user authentication method as claimed in Claim 7, wherein the information processing apparatus and the data holding apparatus are integrated as a unit.

15 9. A user authentication method as claimed in Claim 7, wherein the information processing apparatus has a communication function.

10. A user authentication method as claimed in Claim 5, wherein the data holding apparatus is an IC card.

20 11. A user authentication method as claimed in Claim 9, wherein the data holding apparatus is an IC card.

25 12. A user authentication method as claimed in Claim 11, wherein the information processing apparatus has a communication function, a browser function for accessing information on the Internet, and a reader and writer function for reading and writing the IC card.

30 13. An authentication method, comprising the steps of:  
holding a common key used in a common-key encryption method and a private key used in a public-key encryption method, for each user;  
authenticating, in response to a user authentication request sent from an external information processing apparatus, the user by using the held common key

for the user and a common key used in the common-key encryption method which the user has and is held by a data holding apparatus; and

5 performing, only when the user has been authenticated in the authentication step, processing for making the information processing apparatus authenticate the user by the public-key encryption method by using the private key corresponding to the user.

14. An authentication apparatus, comprising:

a holder for holding a common key used in a common-key encryption method  
10 and a public key used in a public-key encryption method, for each user; and  
an authenticating device for, in response to a user authentication request sent from an external information processing apparatus, authenticating the user by using the common key for the user held by the holder and a common key used in the common-key encryption method for the user held by a data holding medium of the  
15 user, and for, only when the user has been authenticated, performing processing for making the information processing apparatus authenticate the user by the public-key encryption method by using the private key corresponding to the user.

20 15. An authentication apparatus as claimed in Claim 14, wherein the authentication apparatus has a private key used in the public-key encryption method.

16. An authentication apparatus as claimed in Claim 14, wherein the data holding medium is an IC card.

25 17. An authentication apparatus as claimed in Claim 16, wherein the information processing apparatus has a reader and writer function for reading and writing the IC card.

30 18. An authentication apparatus as claimed in Claim 14, wherein the data holding medium is integrated with the information processing apparatus as a unit.

19. An authentication apparatus as claimed in Claim 14, wherein the information processing apparatus is a mobile communication apparatus.
20. An authentication apparatus as claimed in Claim 19, wherein the information processing apparatus has a communication function, and a browser function for accessing information on the Internet.